REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated September 16, 2004. Claims 1-21 are pending. Claims 1-21 are rejected. Claims 1-3, 6-12, and 15-21 have been amended. Accordingly, claims 1-21 remain pending in the present application.

Independent claims 1, 10 and 19 have been amended to recite that the peer-to-peer network includes "at least one server node and a plurality of client nodes, wherein each of the client nodes allow users to publish and share files over the network receive files of the network and search for files to download." The term "node" has been amended to recite "client node" in both the independent and dependent claims. Support for the amendments can be found throughout the Specification, see for example Page 7, lines 11-17; and page 8, lines 15-18. Accordingly, the new matter has been entered.

§102 Rejection

The Examiner rejected claims 1-2, 4-12, and 15-21 under 35 USC §102(b) as being anticipated by non-patent literature "Firewall Design-Here's a practical guide on how to protect your networks" by D. Brent Chapman and Elizabeth D. Zwicky. Applicant respectfully disagrees.

Anticipation requires that the cited reference disclose each and every element of the claimed invention. It is respectfully submitted that the cited article, referred to herein as "Firewall Design," fails to teach or suggest each and every element of the claims.

The present invention provides a peer-to-peer network includes a plurality of computers interconnected over a network, such as the Internet, where some of the

computers are configured as server nodes, and other computers are configured as client nodes. Once content files have been downloaded from the server to client nodes, the client nodes serve the files directly to other client nodes. Typically, the client nodes are created on computers operated by the general public. A user becomes a member of the P2P network by downloading and installing a copy of a P2P client application on the user's computer (page 8, lines 10-16). Once invoked, the P2P client application allows the user to perform four primary functions: publish and share files over the network, receive files over the network, and search for files to download (page 8, lines 15-18). A problem is encountered, however, when one client node attempts to download files from another client node that is protected by a firewall, typically on a private network.

The present invention facilitates file access in the peer-to-peer network by allowing client nodes on the network to serve as proxies to the private networks so that the client nodes inside the private networks can share files over the network through the firewalls (Page 7, lines 11-17). The present invention also reduces cost to operate the P2P by amortizing the cost of the proxies and *not explicitly setting up and maintaining dedicated proxy servers* (Page 4, lines 13-15; and Page, 17, lines 15-17)

Whereas the present invention is capable of turning a client node in the P2P network into a proxy server in order to eliminate the need for dedicated proxy server, Firewall Design is directed to firewall architectures that use dedicated proxy servers.

More specifically, Firewall Design fails to teach or suggest either the definition or the function of the claimed proxy server. First, Firewall Design fails to teach or suggest "designating a first *client node* that is not firewall protected to act as a proxy server, as recited in claim 1. Instead, the "Proxy services" section of Firewall Design (page 3)

explicitly describes proxy services as being a "specialized application or server programs that *run on a firewall host*." On page 4, Firewall Design states: "As the diagram below shows..., the *proxy server runs on the dual-homed host*." Because Firewall Design's teaches the use of a dedicated proxy server that runs on a firewall host, rather than a proxy server created from any client node that is not located behind a firewall, the purpose of which is to eliminate the need for a dedicated proxy server, it is believed that Firewall Design actually teaches away from the present invention.

Another distinction is that the Firewall Design proxy server sits in a location in the network different from the claimed proxy server created from a client node. Page 5 of Firewall Design states that "the "dual-homed host sits between, and is connected to, the Internet and the internal network. In other words, Firewall Design requires that the proxy server run on the firewall host and to sit between the Internet and the internal network of a firewall protected node. Therefore, the Firewall Design proxy server is on the same internal network as the firewall protected node. In the present invention, by contrast, the client node designated as the proxy server (the first client node) does not run on the firewall host and therefore is located external to the internal network of the firewall and the firewall protected node (the second client node). Based on the foregoing, it is clear that the definition of the claimed proxy server is different than the definition of the Firewall Design proxy server.

Not only does the definition of the proxy server of the present invention, which is configured from a client node, different from the definition of the Firewall Design proxy server, but the functions also differ. One of the recited functions of the client nodes of the present invention is to "allow users to publish and share files over the network, receive files over the network, and search for files to download." Because the "proxy

server" is designated from one of the client nodes, the proxy server of the present invention also performs this function. It is respectfully submitted that the Firewall Design proxy server, which is not designated from a client node on the network, but rather runs on a firewall host, fails to perform this function.

Other functions recited in claim 1 of the first client node that is designated as the proxy server include the following: receive an open connection request from the firewall protected second client node (step (c)), receive a request from a third client node for files on the second client node (step (d)), and forward the request to the second client node as a response to the open connection request, thereby allowing other client nodes to access files on the second client node despite the presence of the firewall (step (e)).

Thus, the proxy server of the present invention *receives incoming requests* from the *client nodes on the external network* (Internet) and forwards them to the firewall protected client node on the internal network through the open socket connection. By contrast, Firewall Design describes the proxy service as taking a user's request for Internet services from the internal network and forwarding them to the actual services on an external network. Thus, the Firewall Design proxy server *receives outgoing Internet requests* from a client behind the firewall *on the internal network* and forwards them to a server on an external network, which is opposite from the recitations of the claimed invention.

Because the Firewall Design proxy server fails to meet the definition of the claimed proxy server and fails to perform to the recited functions of the proxy server, the Firewall Design reference fails to teach each and every element of claim 1. Independent claims 10 and 19 include similar recitations. Accordingly, claims 1-2, 4-12, and 15-21 are patentable over Firewall Design.

§103 Rejection

The Examiner rejected claims 3 and 13 under 35 USC §103 (a) as being unpatentable over non-patent literature "Firewall Design-Here's a practical guide on how to protect your networks" in view of US Patent No. 6,052,718 to Gifford.

It is respectfully submitted that a secondary reference stands or falls with the primary reference. Because Firewall Design fails to teach or suggest a method and system for facilitating file access in a peer-to-peer network comprising client nodes, and for designating one of client nodes as a proxy server, that is a network external to the firewall, a combination of Firewall Design with Gifford also fails to teach or suggest the claimed invention. Accordingly, claims 3 and 13 are patentable over the references for at least the same reasons as claims 1, 10 and 19.

The arguments above apply with full force and effect to the remaining dependent claims because they are based on allowable independent claims. Therefore, the dependent claims are allowable for at least the same reasons as the independent claims.

In view of the foregoing, it is submitted that claims 1-21 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-21 as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

March 15, 2005
Date

Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540